

REMARKS

Claims 1-16 are pending in the subject application, wherein independent claim 1 is an apparatus claim and independent claim 9 is a method claim. Claims 1-6 and 9-14 have been amended for clarification. No new matter is presented by the amendments herein.

Rejections under 35 USC §102(e)

The office action rejects claims 1 – 16 under 35 USC §102(e) as being anticipated by U.S. Patent 6,006,332 to Rabne, et al. (hereinafter "Rabne"). However, Applicant contends that Rabne does not, in fact, anticipate the claims of the present application, nor is it particularly similar to the claimed invention structurally or functionally.

Overview of Rabne

Rabne, appears to disclose establishing a specialized *environment* where file transfer and rights management is only possible within that specialized environment. The Abstract of Rabne provides an overview of this specialized, contained environment, which requires at least two specialized client side applications or programs:

[57]

ABSTRACT

A system is provided for controlling access to digitized data. An unsecure client is provided with a launch pad program which is capable of communicating with a secure Rights Management (RM) server. The launch pad program provides an indicator to a public browser, used by the unsecured client, which acknowledges when a rights management controlled object is detected. Once a rights management object is detected, operational control is transferred from the public browser to the launch pad. The launch pad will communicate with the secured RM server and request the digitized data corresponding to the controlled object. In response thereto, the RM server identifies the type of data being requested, i.e. text, audio, video, etc. and transmits this information to the launch pad. The launch pad then searches whether a secure RM browser appropriate to handle this data is resident on the client. When it is determined that no RM browser is resident, the launch pad requests an appropriate browser from the RM server. Based on this request an appropriate RM browser is obtained and authentication and security information are inscribed. Thereafter the RM browser is transmitted to the client. Prior to use, an authentication procedure is undertaken between the launch pad and the RM server to authenticate the RM browser. If authentication does not occur within a predetermined time period, the browser expires.

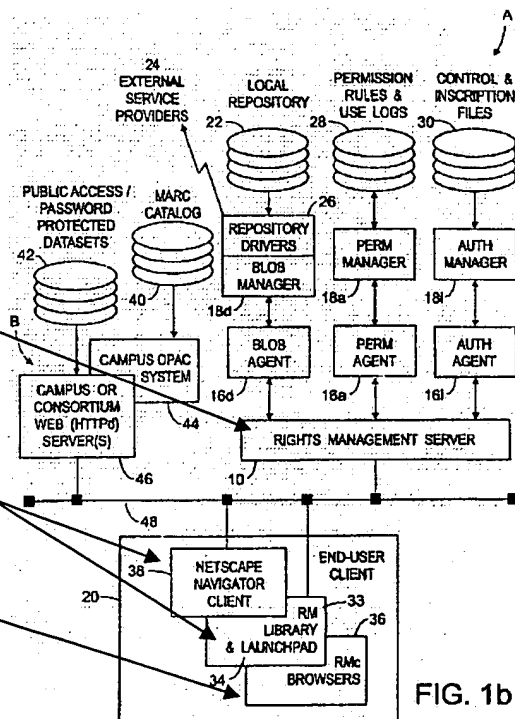


FIG. 1b

The detailed description of Rabne is consistent with its Abstract in describing this environment. Specifically, Rabne provides:

... RM system provides a secure environment for intellectual property management, as illustrated in FIG. 15. Specifically, RM server 10 when an access permission is received, can obtain the intellectual property stored in a secure fashion. This information can be passed to a RMc workstation 20. Once this information is received, RMc browser 36 of the present invention allows various capabilities dependent upon the user ID password and transactions approval.

Col. 22, lines 37-48 (*emphasis added*)

The user is transferred into this environment, to access files from the RM server:

As a user is browsing materials on a Web server, normal HTTP HTML transactions are taking place until the user comes across a pointer to an RM controlled object (i.e. intellectual property). At this point, the user is no longer looking at a standard URL, rather, they are now viewing an RM URL which begins with RM:// rather than the standard HTTP://.

Col. 11, lines 38-44 (*emphasis added*)

The smallest unit of content (or “intellectual property”) available within this environment from the RM server is called a “holding”, which is a file representing one or more catalogued objects in a library.

Holdings: In a library or archive, the *smallest unit that is catalogued* is usually called a holding. Due to the rigors of comprehensive cataloguing, *a holding may be more than one physical object*. A set of slides, or a kit containing several surgical knives may be considered a single holding for catalogue and administration purposes.

Col. 5, lines 24-29 (*emphasis added*)

As discussed by Rabne above, in Rabne’s environment at least two programs are ultimately required at the client side to download files and perform rights management: (1) the launch pad and (2) the rights management (RM) browser.

Launch pad 34 queries RM server 10 to determine the type of media and dispatches the request to the appropriate RMc browser located within RM server 10. RMc browser 36 then downloads the media and provides controlled usage services.

More specifically, Rabne's detailed description further provides for the launch pad:

RM Launch Pad: The RM launch pad enables unsecure WWW browsers to initiate user access to the RM server. Upon startup, the RM launch pad registers an RM URL with the active Web browser. If the WWW browser encounters an RM URL, it forwards that URL to the launch pad application for processing. *The launch pad determines what kind of browser or browsers are required to process the requested URL. The appropriate RMc browser is downloaded to the workstation, and the RM launch pad passes execution control and the requested holding and/or element data to the RMc browser.*

Col. 6, line 61 – col. 7, line 4 (*emphasis added*)

And Rabne provides with respect to the RM Browser:

Rights Manage Compliant Browsers: Publishers expressed a need to protect intellectual property once it has been transmitted from a trusted server (i.e. RM server) to a user's workstation. The workstation must therefore contain *a trusted program that can securely receive intellectual property, prevent unauthorized uses of it, and report all authorized uses to the RM server. Applications that adhere to these security principles are referred to as Rights Manager-compliant (RMc).* The RM Server and RMc browsers communicate with a protocol that specifies the format of commands that are exchanged and the security measures required to protect intellectual property. *Communications between the RM server and any RMc browser must be encrypted to protect the intellectual property during network transmission.*

Col. 6, lines 31-45 (*emphasis added*)

Secure requests require "an encrypted private channel." (Col. 6, lines 31-45, Col. 11, lines 59-61) And communications between the launch pad or RM browser (as indicated above) and RM server requires a proprietary protocol. (Col. 6, lines 31-45, Col. 12, lines 10-14)

In Rabne's environment only the RM browser(s) can access content. And different specialized browsers are required for different types of files (e.g., text, audio, video). See, for example FIG. 2 (e.g., browsers 36a and 36b) and the following:

The only way to access the many types of information available from the RM server is via an RMc browser application. Each RMc browser may handle a single simple content type (text, image, audio, video, catalog, collection), or multiple simple types. RMc

browsers may also present complex content types composed of a holding of heterogenous elements (e.g., Musical Scores, Art Museum material, class syllabus, scientific journals).

Col. 6, lines 53-60 (*emphasis added*)

Perhaps as an inherent characteristic of the Rabne environment, it is the RM browsers (i.e., applications) that enforce rights management, as is clearly shown in Rabne's Fig. 15 and as discussed in the below text:

As previously discussed, *RMc browsers* are trusted clients which *not only deal with permissions but enforce the functionality that is available to a user*. Particularly, RMc browsers will "gray out" in a Windows environment things such as a capability to print, download, etc. if a user does not have those sort of rights or permissions. Therefore, use of RMc browsers are an active engagement.

Col. 20, lines 17-18 (*emphasis added*)

Once this information is received, RMc browser 36 of the present invention allows various capabilities dependent upon the user ID password and transactions approval. Specifically, depending upon the level of access, etc. *the browser will provide various permissions such as a display, play, local print permission, download permission or clip permission, etc.*

Col. 22, lines 42-48 (*emphasis added*)

In the Rabne system and environment, once the RM browser is no longer required – it is automatically removed. (Col. 13, lines 38-46)

Discussion

There are, therefore, several fundamental contrasts between the presently claimed invention and the "secure environment" taught by Rabne, which demonstrate that Rabne does not anticipate, for example, claim 1 (as amended herein) of the present application.

1) Rabne does not enforce rights at the *OS kernel level*, as required by presently amended claim 1. Thus, Rabne does not anticipate this claim. For example, the present application provides that "policy is enforced within the kernel of the OS", which allows for "trapping of kernel-level OS calls". (See Present Application, p. 31, line 14 p.37, line 4; Fig. 2; Fig. 4) In contrast, Rabne uses a temporary RM browser *application* to enforce rights, as is indicated in the Rabne excerpts above. Therefore, unlike the client module of the present

application, as an application Rabne's RM browser executes on top of the client's OS – like any other application. As such, Rabne's enforcement is at the application level, not the OS level, or within the OS kernel. Rabne's browser is, therefore, quite different from the client module of the present invention. For example, since applications and programs run above the operating system, not within the operating system, "trapping of kernel-level OS calls" as in the present invention is not taught by Rabne. Since Rabne does not enforce rights at the OS level, Rabne does not anticipate claim 1.

2) Rabne does not anticipate accessing content within a native application for the content. Rather, Rabne teaches its own "environment" within which its files are retrieved, transmitted and then accessed via the RM browser. This environment is significantly different from the more flexible approach posed in the present application, and, as a result, the limitations inherent in Rabne's environment are avoided. In the present invention, the content can be accessed within the context of its native application (e.g., MS Word), since the rights are enforced at the OS level. But in Rabne rights are enforced by the RM browser, so it appears that content can not be accessed within its native application, see the above excerpts.

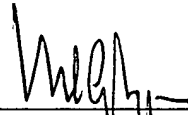
3) Rabne does not operate on **data blocks**, as in amended claim 1. Specifically, it has been made clear in claim 1 that the present invention can operate on data blocks, i.e., blocks of data (or content) that may be smaller than files. Rabne does not discuss this at all. Rather, Rabne teaches operating on files (e.g., text, video, audio) with the smallest of such files referred to as a "holding" that represents an object. In fact, Rabne is so reliant on files, that even the type of RM browser that is downloaded from the RM server is chosen based on the type of file that has been requested. For instance, a text RM browser may be downloaded for text files and an image RM browser may be downloaded for image files, as shown in Rabne's Fig. 2. As reflected by the content component of amended claim 1, the present invention teaches that the content may be separated into blocks – rather than a complete file. Blocks can be individually evaluated and transmitted, and encrypted. (See Present Application, p. 57, line 10 p. 63, line 17) However, Rabne teaches only transmission of the entire files (e.g., audio, video, text) within its environment, but does not teach operating on data blocks within those files. Therefore, this aspect of claim 1 is not anticipated by Rabne. Accordingly, Applicant respectfully requests removal of the rejection to claim 1.

For the reasons set forth above, Applicant contends that claim 1 is not anticipated in light of the cited references. Accordingly, Applicant respectfully requests withdrawal of the rejection of claim 1. For the same reason, Applicant also requests withdrawal of the rejections to claims 2-8, which depend from claim 1.

Independent claim 9 has been amended consistent with the amendments of claim 1. Thus, for the same reasons set forth for claim 1, Applicant also contends that independent claim 9 is not anticipated by the cited reference and respectfully requests removal of those rejections and removal of the rejections to its respective dependent claims 10-16.

Beyond the Three Month Extension requested, no additional costs are believed to be due in connection with the filing of this disclosure. However, the Commissioner is hereby authorized to charge any additional fees under 37 C.F.R. §1.16 and §1.17 that may be required, or credit any overpayment, to our Deposit Account No. 50-1133.

Respectfully submitted,



Mark G. Lappin, Reg. No. 26,618
McDermott, Will & Emery
28 State Street
Boston, MA 02109
Tel (617) 535-4037
Fax (617) 535-3800

Date: July 5, 2005